

REMARKS

This amendment is responsive to the Office Action of February 25, 2009. Reconsideration and allowance of **claims 1-5 and 7-38** are requested.

The Office Action

Claims 1, 9, 16 and 24 were objected to due to minor informalities.

Claim 1, 9, 24, and 32 were rejected under 35 U.S.C. 101.

Claims 1, 9, 16, 24, and 32 were rejected under 35 U.S.C. 112, first paragraph.

Claims 1, 9, 16, 24, and 32 were rejected under 35 U.S.C. 112, second paragraph.

Claims 1-5, 9-12, and 14 were rejected under 35 U.S.C. 102(b) over Maurer (EP 0511420).

Claims 8 and 15 were rejected under 35 U.S.C. 103(a) over Maurer in view of van Someren (US Patent Application Publication 2008/0044027).

Claims 6, 13, 16, 24, and 32 were indicated as containing allowable subject matter.

The Present Application

The present application is directed a system and method of reliable forward secret key sharing with physical random functions. The present application discloses a system and method of reliable forward secret key sharing between two legitimate correspondents whose profiles match sufficiently. The method relies on a physical random function to provide a secure solution to reliable forward secret key sharing.

The above description of the present application is presented to the Examiner as background information to assist the Examiner in understanding the application. The above description is not used to limit the claims in any way.

Claim Objections

Claims 1, 9, 16, and 24 have been amended to address the Examiner's objections.

35 U.S.C 101

Claims 1, 9, 16, 24, and 32 have been amended to address the Examiner's rejections.

35 U.S.C. 112, 1st Paragraph

The Office Action asserts that the claims **1, 9, 16, 24, and 32** contain subject matter which is not described in the specification in such a way as to enable one skilled in the art to which it pertain. The Examiner asserts that there are two enablement issues that are not disclosed in the specification: 1) how to generate a codeword W from the (d-1) parity symbol and the response B and 2) how to determine the secret key K from the generated codeword W.

As per the first issue, it is respectfully submitted that generating a codeword W' from the (d-1) parity symbol and the response B is disclosed in the specification. More specifically, page 8, lines 12-19 discloses that in reconstructing the codeword W, Reed-Solomon decoding is used to construct a word W' which includes question marks in the first k positions, followed by the symbol sequence B (from challenge-response pair (C,B)) in the next n positions, and the parity symbols P in the last (d-1) positions. Additionally, page 18, lines 4-14 discloses the processor constructs the word W' by including question marks (?) on the k positions corresponding to the secret key K. Next, the symbol sequence of the B is placed in the next n positions of word W'. Finally, the transmitted parity information, i.e., the (d-1) parity symbols P are added to the last part of the word W'. The word W' is then supplied as input to a Reed-Solomon decoder in the computer to reconstruct the original codeword, W, as described above to extract the secret key K.

As per the second issue, it is respectfully submitted that determining the secret key K from the generated codeword W' is disclosed in the specification. More specifically, page 8, line 21 through page 9, line 10 discloses that the secret key K is determined when a second correspondent receives the parity symbols transmitted as the redundant information over the public channel from the first correspondent and performs Reed-Solomon decoding to reconstruct W. The processor reconstructs codeword W by constructing a word W' that includes question marks (?) on the k positions corresponding to the secret key K. Next, the symbol sequence of the B is placed in the next n positions of word W'. Finally, the transmitted parity information, i.e., the (d-1) parity symbols P are added to the last part of the word W'. The word W'

is then supplied as input to a Reed-Solomon decoder in the computer to reconstruct the original codeword, W. The reconstructed original codeword contains the secret key K which is then extracted and used by the second correspondent.

35 U.S.C. 112, 2nd Paragraph

Claims 1, 9, 16, 24, and 32 have been amended to address the Examiner's rejections.

The Claims Are Now In Condition for Allowance

Claim 1 has been amended to incorporate the subject matter of **claim 6**, which has been indicated as containing allowable subject matter. Additionally, **claim 1** has been amended to overcome the rejections under 35 U.S.C. 101, 35 U.S.C. 112, 1st paragraph, and 35 U.S.C. 112, 2nd paragraph. Accordingly, it is submitted that **claim 1** and **claims 2-5 and 7-8** are now in condition for allowance.

Claim 9 has been amended to incorporate subject matter from **claim 13**, which has been indicated as containing allowable subject matter. Additionally, **claim 9** has been amended to overcome the rejections under 35 U.S.C. 101, 35 U.S.C. 112, 1st paragraph, and 35 U.S.C. 112, 2nd paragraph. Accordingly, it is submitted that **claim 9** and **claims 10-15** are now in condition for allowance.

Claim 16 has been amended to overcome the rejections under 35 U.S.C. 101, 35 U.S.C. 112, 1st paragraph, and 35 U.S.C. 112, 2nd paragraph. Accordingly, it is submitted that **claim 16** and **claims 17-23** are now in condition for allowance.

Claim 24 has been amended to overcome the rejections under 35 U.S.C. 101, 35 U.S.C. 112, 1st paragraph, and 35 U.S.C. 112, 2nd paragraph. Accordingly, it is submitted that **claim 24** and **claims 25-31** are now in condition for allowance.

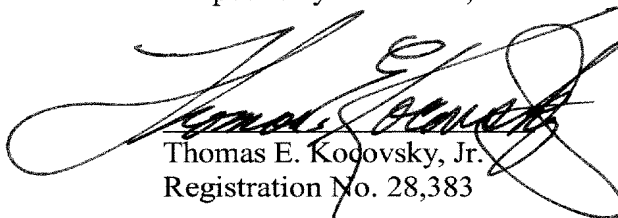
Claim 32 has been amended to overcome the rejections under 35 U.S.C. 101 and 35 U.S.C. 112, 2nd paragraph. Accordingly, it is submitted that **claim 32** and **claims 33-38** are now in condition for allowance.

CONCLUSION

For the reasons set forth above, it is submitted that **claims 1-5 and 7-38** (all claims) distinguish patentably over the references of record and meet all statutory requirements. An early allowance of all claims is requested.

In the event the Examiner considers personal contact advantageous to the disposition of this case, the Examiner is requested to telephone Thomas Kocovsky at 216.363.9000.

Respectfully submitted,



Thomas E. Kocovsky, Jr.
Registration No. 28,383

FAY SHARPE LLP
The Halle Building, 5th Floor
1228 Euclid Avenue
Cleveland, OH 44115-1843
Telephone: 216.363.9000 (main)
Telephone: 216.363.9122 (direct)
Facsimile: 216.363.9001
E-Mail: tkocovsky@faysharpe.com

Direct All Correspondence to:
Yan Glickberg, Reg. No. 51,742
P.O. Box 3001
Briarcliff Manor, NY 10510-8001
(440) 483-3455 (tel)
(440) 483-2452 (fax)